

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-166996

(43)Date of publication of application : 22.06.2001

(51)Int.Cl.

G06F 12/14  
G09C 1/00  
G11B 20/10  
H04L 9/10  
H04L 9/32

(21)Application number : 2000-252462

(71)Applicant : MATSUSHITA ELECTRIC IND CO  
LTD  
TOSHIBA CORP

(22)Date of filing : 23.08.2000

(72)Inventor : HARADA TOSHIHARU  
TATEBAYASHI MAKOTO  
KOZUKA MASAYUKI  
HIROTA TERUTO  
KAMIBAYASHI TATSU  
TAMURA MASABUMI

(30)Priority

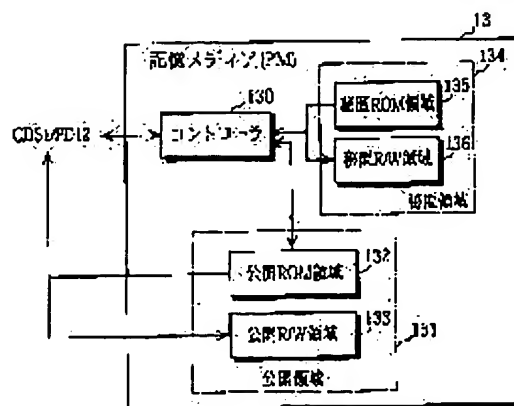
Priority number : 1999 436035 Priority date : 08.11.1999 Priority country : US

(54) STORAGE MEDIUM AND METHOD AND DEVICE FOR UPDATING REVOCATION INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a storage medium or the like for excluding any access to contents in respect to illegal electronic equipment generated afterwards.

SOLUTION: A storage media (PM) 13 is provided with a controller 130 and two kinds of storage areas (a secret area 134 and a public area 131). The public area 131 is provided with a public R/W area 133 for storing digital contents and a public ROM-W area 132a for storing the identification information of electronic equipment being the object of the inhibition of any access to the digital



This Page Blank (uspto)

contents as revocation information, and a public ROM area 132 for storing the identification information of the electronic equipment being the object of the inhibition of the update of the revocation information as master revocation information. When this storage medium is mounted on the electronic equipment having the identification information registered in the public ROM area 132, the controller 130 rejects the update of the revocation information by the electronic equipment.

---

## LEGAL STATUS

[Date of request for examination] 28.11.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3312024

[Date of registration] 24.05.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

This Page Blank (uspto)

特開 2001-166996

(P2001-166996A)

(43) 公開日 平成13年6月22日(2001.6.22)

(51) Int. Cl. 7	識別記号	F I	メモコード(参考)
G 0 6 F	12/14	3 1 0	K
		3 2 0	A
G 0 9 C	1/00	6 6 0	D
G 1 1 B	20/10		H
H 0 4 L	9/10	6 2 1	A
審査請求	未請求	請求項の数 19	O L
			(全 17 頁) 最終頁に続く

(21) 出願番号 特願2000-252462(P2000-252462)

(22) 出願日 平成12年8月23日(2000.8.23)

(31) 優先権主張番号 09/436035

(32) 優先日 平成11年11月8日(1999.11.8)

(33) 優先権主張国 米国(US)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 原田 俊治

大阪府門真市大字門真1006番地

松下電器

産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗 (外1名)

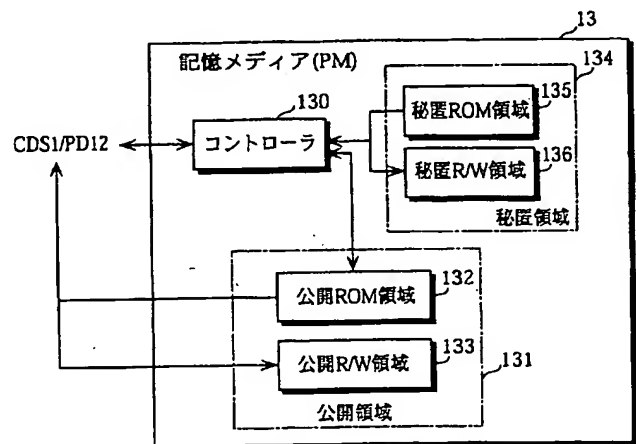
最終頁に続く

(54) 【発明の名称】 記憶媒体、リボケーション情報更新方法及び装置

(57) 【要約】

【課題】 後発的に発生した不正な電子機器に対しても、コンテンツへのアクセスを排除することが可能な記憶媒体等を提供する。

【解決手段】 記憶メディア(PM) 13は、コントローラ130と2種類の記憶領域(秘匿領域134及び公開領域131)とを有する。公開領域131は、デジタルコンテンツを記憶するための公開R/W領域133と、そのデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報をリボケーション情報として記憶するための公開ROM-W領域132aと、そのリボケーション情報の更新を禁止する対象となる電子機器の識別情報をマスタリボケーション情報として記憶している公開ROM領域132とを備える。コントローラ130は、公開ROM領域132に登録された識別情報を有する電子機器に装着された場合には、その電子機器によるリボケーション情報の更新を拒否する。



## 【特許請求の範囲】

【請求項1】 電子機器に装着されて使用される記憶媒体であって、

デジタルコンテンツを記憶するためのコンテンツ記憶領域と、

前記コンテンツ記憶領域に記憶されたデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報に対応する情報をリボケーション情報として記憶するためのリボケーション情報記憶領域と、

前記リボケーション情報記憶領域に記憶されるリボケーション情報の更新を禁止する対象となる電子機器の識別情報に対応する情報をマスターボケーション情報として記憶しているマスターボケーション情報記憶領域とを備えることを特徴とする記憶媒体。

【請求項2】 前記記憶媒体は、さらに、

当該記憶媒体が装着された電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへの前記電子機器によるアクセスを許可するコンテンツ保護手段と、

前記電子機器の識別情報が前記マスターボケーション情報記憶領域に記憶されたマスターボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記電子機器からの指示に従って、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新するリボケーション情報更新手段とを備えることを特徴とする請求項1記載の記憶媒体。

【請求項3】 前記マスターボケーション情報記憶領域は、予めマスターボケーション情報が記憶されたROMであることを特徴とする請求項2記載の記憶媒体。

【請求項4】 前記記憶媒体は、さらに、

前記リボケーション情報更新手段によるリボケーション情報の更新の可否判断に先立って、前記電子機器と相互認証をし、相互認証に成功した場合にのみ前記電子機器と共有し合うことができる秘密鍵を生成する相互認証手段を備え、

前記リボケーション情報更新手段は、前記相互認証手段が生成した秘密鍵を用いて前記リボケーション情報を更新することを特徴とする請求項2記載の記憶媒体。

【請求項5】 前記リボケーション情報更新手段は、前記識別情報が前記マスターボケーション情報に対応する識別情報に該当しないと判断した場合には、前記電子機器がリボケーション情報を更新するために必要となる秘密鍵を前記電子機器に送信することを特徴とする請求項2記載の記憶媒体。

【請求項6】 前記リボケーション情報記憶領域は、複数のグループに分類してリボケーション情報を記憶するための複数の記憶領域を有し、

前記リボケーション情報更新手段は、当該記憶媒体に装着された電子機器の識別情報が前記マスターボケーション情報記憶領域に記憶されたマスターボケーション情報に対応する識別情報に該当しないと判断し、かつ、前記電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報のうち前記電子機器が更新しようとしているグループに属するリボケーション情報に対応する識別情報に該当しないと判断した場合に、前記グループに属するリボケーション情報だけを更新することを特徴とする請求項2記載の記憶媒体。

【請求項7】 前記リボケーション情報記憶領域は、前記デジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をリボケーション情報として記憶し、前記コンテンツ保護手段は、前記リボケーション情報記憶領域に記憶されたリボケーション情報を当該記憶媒体が装着された電子機器に送信し、それに対する前記電子機器からの返信情報が一定の規則性を有するか否かを判断することによって、当該電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断し、前記マスターボケーション情報記憶領域は、前記リボケーション情報の更新を禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をマスターボケーション情報として記憶し、

前記リボケーション情報更新手段は、前記マスターボケーション情報記憶領域に記憶されたマスターボケーション情報を当該記憶媒体が装着された電子機器に送信し、それに対する前記電子機器からの返信情報が一定の規則性を有するか否かを判断することによって、前記電子機器の識別情報が前記マスターボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断するを備えることを特徴とする請求項2記載の記憶媒体。

【請求項8】 請求項1記載の記憶媒体のリボケーション情報を更新する方法であって、記憶媒体が電子機器に装着されたことを検出する検出ステップと、

前記電子機器が有する第1の識別情報が前記記憶媒体のマスターボケーション情報記憶領域に記憶されたマスターボケーション情報に対応する識別情報に該当するか否かを判断する判断ステップと、  
該当しないと判断された場合にのみ、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新する更新ステップとを含むことを特徴とするリボケーション情報更新方法。

【請求項9】 前記更新ステップでは、前記電子機器が有する第2の識別情報に対応する情報を新しいリボケーション情報として前記リボケーション情報記憶領域に記憶させることを特徴とする請求項8記載のリボケーシ

10

20

30

40

50

ン情報更新方法。

【請求項10】 前記リボケーション情報更新方法は、さらに、

前記電子機器と前記記憶媒体とが相互認証をし、相互認証に成功した場合にのみ前記電子機器と前記記憶媒体とが共有し合うことができる秘密鍵を生成する相互認証ステップを含み、

前記更新ステップでは、前記相互認証ステップで生成された秘密鍵を用いて前記リボケーション情報を更新するを含むことを特徴とする請求項9記載のリボケーション情報更新方法。

【請求項11】 前記更新ステップは、

前記第1の識別情報が前記マスタリボケーション情報に対応する識別情報に該当しないと判断した場合に、前記相互認証で共有された秘密鍵を用いて、前記第2の識別情報に対応する情報を新しいリボケーション情報として暗号化した後に、前記電子機器から前記記憶媒体に転送するサブステップと、

転送されてきた前記第2の識別情報に対応する情報を前記秘密鍵で復号化した後に、前記リボケーション情報記憶領域に記憶させるサブステップとを含むことを特徴とする請求項10記載のリボケーション情報更新方法。

【請求項12】 前記判断ステップは、さらに、前記第2の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に該当するか否かを判断するサブステップを含み、

前記更新ステップでは、前記判断ステップにおいて、前記第1の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しないと判断され、かつ、前記第2の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に該当しないと判断された場合に、前記第2の識別情報に対応する情報を新しいリボケーション情報として前記リボケーション情報記憶領域に記憶させることを特徴とする請求項9記載のリボケーション情報更新方法。

【請求項13】 前記マスタリボケーション情報記憶領域は、前記リボケーション情報の更新を禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をマスタリボケーション情報として記憶し、

前記判断ステップでは、前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報を当該記憶媒体が装着された電子機器に送信し、それに対する前記電子機器からの返信情報が一定の規則性を有するか否かを判断することによって、前記電子機器が有する第1の識別情報が前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当するか否かを判断することとを特徴とする請求項9記載のリボケーション情報更新方法。

【請求項14】 請求項1記載の記憶媒体のリボケーション情報を更新する装置であって、

前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しない第1の識別情報を記憶している第1識別情報記憶手段と、

前記第1記憶情報記憶手段に記憶された第1の識別情報に対応する情報を用いて、前記記憶媒体から、前記記憶媒体に記憶されるリボケーション情報を更新する許可を取得する許可取得手段と、

取得した許可に従って前記記憶媒体に記憶されるリボケーション情報を更新する更新手段とを備えることを特徴とするリボケーション情報更新装置。

【請求項15】 前記更新手段は、予め記憶している第2の識別情報に対応する情報を用いて前記リボケーション情報を更新することを特徴とする請求項14記載のリボケーション情報更新装置。

【請求項16】 前記リボケーション情報更新装置は、さらに、

20 前記記憶媒体による前記リボケーション情報の更新の可否判定に先立って、前記記憶媒体と相互認証をし、相互認証に成功した場合にのみ前記記憶媒体と共有し合うことができる秘密鍵を生成する相互認証手段を備え、

前記更新手段は、前記相互認証で共有された秘密鍵を用いて、前記リボケーション情報を更新することを特徴とする請求項15記載のリボケーション情報更新装置。

【請求項17】 前記更新手段は、前記相互認証で共有された秘密鍵を用いて、前記第2の識別情報に対応する情報を新しいリボケーション情報として暗号化した後に、前記電子機器から前記記憶媒体に転送することによって、前記リボケーション情報を更新することを特徴とする請求項16記載のリボケーション情報更新装置。

【請求項18】 前記リボケーション情報記憶領域は、複数のグループに分類してリボケーション情報を記憶するための複数の記憶領域を有し、

前記更新手段は、前記第2の識別情報に対応する1つのグループに属するリボケーション情報だけを更新することとを特徴とする請求項15記載のリボケーション情報更新装置。

40 【請求項19】 前記マスタリボケーション情報記憶領域は、前記リボケーション情報の更新を禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をマスタリボケーション情報として記憶し、

前記許可取得手段は、前記記憶媒体から送信されてくるマスタリボケーション情報を受信し、前記第1の識別情報で復号化した後に、その復号結果と一定の規則性を有する情報を前記記憶媒体に返信することによって前記許可を取得することを特徴とする請求項15記載のリボケーション情報更新装置。

## 【発明の詳細な説明】

## 【０００１】

【発明の属する技術分野】本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタルコンテンツを格納しておくための記憶媒体、不当な電子機器によるデジタルコンテンツの記録や再生を抑止するのに用いられるリボケーション情報を更新する方法及び装置に関する。

## 【０００２】

【従来の技術】近年、デジタル技術やマイクロプロセッサ応用技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤ、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【０００３】これらのデジタルコンテンツは、例えば、MPEG2、MP3といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。しかしながら、パーソナルコンピュータ、セットトップボックス、プレーヤなどの電子機器で用いられる記憶媒体は、別の電子機器に移動しても記録再生できるリバーシブルなものが多く、その仕様は基本的にオープンである。このため、コンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは実際上困難である。

【０００４】そこでメモ리카ードのように記憶メディア部とコントローラが一体化された記憶媒体については、コントローラによるアクセス制御機能によって、秘匿された特定手続きでのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことで、コンテンツの保護を図ることが考えられる。

【０００５】この場合、パーソナルコンピュータ、セットトップボックス、プレーヤなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互認証し、正しいと認められた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。

## 【０００６】

【発明が解決しようとする課題】ところが、上述のような著作権保護のための仕組み（例えば相互認証に必要な情報やプログラム等）は、電子機器の出荷段階で予め設定されていることから、機器の購入後に当該電子機器（上で動作するプログラム等）が改変されるといった攻撃によってコンテンツ保護の仕組みが無用のものになってしまう場合においては、もはや、相互認証だけではこの種の不正な電子機器を検出して排除することができず、著作権は侵害されてしまう。

10 【０００７】この対策として、いわゆるブラックリストとしてのリボケーション情報、即ち、記憶媒体に格納されているコンテンツへのアクセスを禁止する対象となる電子機器（の識別情報の一覧）を示すリボケーション情報を記憶媒体の特定記憶領域に予め登録しておき、このような記憶媒体が、リボケーション情報として登録された電子機器に装着して使用されようとした場合に、その電子機器の当該記憶媒体へのアクセスを禁止する、つまり、当該記憶媒体へのアクセス権を無効化することによってコンテンツの保護を図ることも考えられる。

20 【０００８】ところが、このような方策であっても、リボケーション情報自体は記憶媒体の出荷段階において書き換え不可能な記憶領域等に登録される必要があることから、当該記憶媒体の出荷後において、ある電子機器（上で動作するプログラム）の改変が行われた場合には、そのような不正な電子機器をリボケーション情報に追加登録することができないために、やはり、この種の電子機器による不正なアクセスを排除できない。

30 【０００９】そこで、本発明は、上記事情を考慮してなされたものであり、リボケーション情報を参照することによって不正な電子機器によるコンテンツへのアクセスを排除する機能を有する記憶媒体であって、後発的に発生した不正な電子機器に対しても、コンテンツへのアクセスを排除することが可能な記憶媒体、そのためのリボケーション情報更新方法及び装置を提供することを目的とする。

## 【００１０】

40 【課題を解決するための手段】上記目的を達成するために、電子機器に装着されて使用される記憶媒体であって、デジタルコンテンツを記憶するためのコンテンツ記憶領域と、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報に対応する情報をリボケーション情報として記憶するためのリボケーション情報記憶領域と、前記リボケーション情報記憶領域に記憶されるリボケーション情報の更新を禁止する対象となる電子機器の識別情報に対応する情報をマスタリボケーション情報として記憶しているマスタリボケーション情報記憶領域とを備えることを特徴とする。

50 【００１１】また、本発明に係るリボケーション情報更新方法は、上記記憶媒体のリボケーション情報を更新す



る方法であって、記憶媒体が電子機器に装着されたことを検出する検出ステップと、前記電子機器が有する第1の識別情報が前記記憶媒体のマスタリポケーション情報記憶領域に記憶されたマスタリポケーション情報に対応する識別情報に該当するか否かを判断する判断ステップと、該当しないと判断された場合にのみ、前記リポケーション情報記憶領域に記憶されるリポケーション情報を更新する更新ステップとを含むことを特徴とする。

【0012】さらに、本発明に係るリポケーション情報更新装置は、上記記憶媒体のリポケーション情報を更新する装置であって、前記記憶媒体のマスタリポケーション情報記憶領域に記憶されたマスタリポケーション情報に対応する識別情報に該当しない第1の識別情報を記憶している第1識別情報記憶手段と、前記第1識別情報記憶手段に記憶された第1の識別情報に対応する情報を用いて、前記記憶媒体から、前記記憶媒体に記憶されるリポケーション情報を更新する許可を取得する許可取得手段と、取得した許可に従って前記記憶媒体に記憶されるリポケーション情報を更新する更新手段とを備えることを特徴とする。

【0013】つまり、記憶媒体の特定の記憶領域に、コンテンツへのアクセスを禁止すべき1つ以上の電子機器を特定するリポケーション情報と、当該リポケーション情報を更新することが特別に許可された電子機器を特定する（特別なリポケーション情報である）マスタリポケーション情報とを予め登録した構成とし、これによって、当該記憶媒体が、当該マスタリポケーション情報で表される電子機器に装着して使用された場合に、リポケーション情報の更新を許可する。

【0014】具体的には、記憶メディア（PM）は、コントローラと2種類の記憶領域（秘匿領域及び公開領域）とを有する。公開領域は、デジタルコンテンツを記憶するための公開ROM領域と、そのデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報をリポケーション情報として記憶するための公開ROM領域と、そのリポケーション情報の更新を禁止する対象となる電子機器の識別情報をマスタリポケーション情報として記憶している公開ROM領域とを備える。コントローラは、公開ROM領域にマスタリポケーション情報として登録された識別情報を有する電子機器に装着された場合には、その電子機器によるリポケーション情報の更新を拒否する。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図1は、本実施の形態における著作権保護システム100の構成要素を示す図である。この著作権保護システム100は、電子配信や記録媒体により流通されるデジタル著作物の著作権を保護するシステムであり、インターネットや放送等の通信網を介して音楽コンテンツを電子配信する自動販売機である

コンテンツ販売システム（CONTENT DISTRIBUTE SYSTEM（CDS））1と、音楽コンテンツを格納しておくための記憶メディア（PORTABLE MEDIA（PM））13、PM13に音楽コンテンツを記録したりPM13に記録された音楽コンテンツを再生するための携帯型の記録再生装置（PORTABLE DEVICE（PD））12と、音楽コンテンツを記録・再生・移動等によって管理をする装置であるコンテンツ利用管理システム（LICENSE COMPLIANT MODULE（LCM））21から構成される。

10 【0016】これらCDS1、PM13及びPD12は、上述したリポケーション情報を更新することによって、後発的に発生した不正な電子機器であっても、そのような電子機器によるデジタル著作物への不正なアクセスを排除することができる機能や構造を有している。図2は、CDS1の構成を示すブロック図である。ここで、ELECTRONIC MUSIC DISTRIBUTOR（EMD）40は、音楽配信サーバや音楽放送局等であり、リポケーション情報発行機関（REVOCATION INFORMATION LICENSING ENTITY（RLE））41は、不正な電子機器が新たに判明した場合等において、その電子機器の識別情報を含む新たなリポケーション情報を発行する機関（コンピュータ等）である。

20 【0017】CDS1は、例えば、レコード店等に置かれる専用端末（KIOSK端末）等として実現されるものであり、EMD40及びRLE41と伝送路で接続され、セキュア・コンテンツ・サーバ（SECURE MUSIC SERVER（SMS））2、EMD\_I/F（INTERFACE）部3、PD\_I/F部5、メディア\_I/F部6、秘匿領域ドライバ7、宿帳格納部8、ライセンス格納部9、音楽データ格納部10、リポケーション情報受信部14、ユーザ\_I/F部15、リポケーション情報格納部16から構成され、以下の機能を有する。

30 【0018】（1）コンテンツの記録（購入）機能  
装着されたPM13に、利用者が指定したコンテンツを記録（購入）する。

（2）リポケーション情報の更新機能  
装着されたPM13に、無効化すべき電子機器を示すリポケーション情報を記録し更新する。

40 【0019】EMD\_I/F部3は、複数のEMD40と接続するための通信アダプタ等であり、PD\_I/F部5は、PD12と接続するUSB（UNIVERSAL SERIAL BUS）等であり、メディア\_I/F部6は、PM13を装着するためのPCMCIA用のカードスロット等であり、リポケーション情報受信部14は、RLE41から、登録すべき新たなリポケーション情報を受信する通信アダプタ等であり、ユーザ\_I/F部15は、LCDやスイッチ・ボタンキー等である。

50 【0020】音楽データ格納部10は、暗号化された音楽コンテンツを格納するためのフラッシュメモリ等であり、宿帳格納部8は、音楽データ格納部10に格納された音楽コンテンツの属性情報等を格納するためのメモリ等であり、ライセンス格納部9は、音楽データ格納部10に格納された暗号化音楽コンテンツを復号するための

鍵等を格納するためのメモリ等であり、リボケーション情報格納部16は、RLE41等から受信したリボケーション情報を一時的に格納しておくためのメモリ等である。

【0021】秘匿領域ドライバ7は、ユーザには公開されていない秘匿された手順で宿帳格納部8等の後述する秘匿領域の記憶領域に対して、ユーザには公開されていない特定手順でアクセスする制御回路等であり、SMS2は、これら構成要素を制御することで上述の2つの機能を発揮する処理を実行するCPU等である。以下、CDS1の各構成要素の機能及びSMS2の制御内容を、上記

(1)、(2)の機能毎に説明する。

【0022】(1) コンテンツの記録(購入)機能  
CDS1におけるコンテンツ保護の方法は、コンテンツを記録すべきPM13毎にその記憶メディアの識別情報(メディアID)を用いてコンテンツの暗号化/復号化を行うことを前提としている。CDS1は、複数のEMD40(ここでは、EMD11~13)に対応した受信部11~13を有しており、当該受信部11~13を通してEMD40が配信する暗号化コンテンツ(ここでは音楽コンテンツ)またはライセンス情報(利用条件、暗号化コンテンツ復号キーなど)を受信する。ここで各EMD40が配信する暗号化コンテンツは、それぞれ独立の暗号方式や、音声圧縮符号化方式を用いて作成されている。受信部11~13は再生機能や課金機能を有していても良い。また、利用者は、課金機能を利用して、気に入ったコンテンツを購入することが可能である。

【0023】SMS2は、利用者が購入した暗号化コンテンツをEMD11/F部3を経由して受け取る。このとき、暗号化コンテンツ(即ち、各EMD40毎に独立の暗号方式や音声圧縮方式で作成された暗号化コンテンツ)は、必要に応じて、EMD11/F部3で復号され、CDS1において音声圧縮符号化方式や暗号方式への変換(再暗号化)が施される。

【0024】SMS2は暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、暗号化コンテンツを復号するための鍵(暗号化コンテンツ復号キー)をライセンス格納部9に格納する。ここでSMS2は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、SMS2が管理する音楽コンテンツをCDS1上で再生することができる。

【0025】SMS2は、また、メディア1/F部6に装着可能なメモリカード等のPM13に対して、音楽データ格納部に格納された暗号化コンテンツ(音楽コンテンツ)を当該1/F部6経由で出力する機能を有している。PM13は、PD12上にセットして用いることで、当該PM13に記録された暗号化コンテンツ(音楽コンテンツ)をPD12上で復号し再生することができる。SMS2からPM13へのコンテンツの記録は、メディア1/F部6を通じて直接行われるか、またはPD12を経由して行うことができ

る。また、このPM13は、LCM21にセットして用いることで、当該PM13に記録された暗号化コンテンツ(音楽コンテンツ)を、LCM21上で復号し再生したり、LCM21上に暗号化コンテンツ(音楽コンテンツ)を移動させて保管することができる。

【0026】(2) リボケーション情報更新機能

リボケーション情報は、コンテンツ保護のためにPM13の利用(PM13へのコンテンツの記録、PM13からのコンテンツの読み出しや再生など)を無効化すべき電子機器(PD、LCM)が判別可能な情報であり、PM13に、出荷段階で予め登録されている。

【0027】リボケーション情報更新機能は、この出荷段階で登録されたリボケーション情報を、必要に応じて(すなわち、新たに無効化すべき機器が発生した場合に)、特別に許可された電子機器(ここではCDS1)を通じて、新しいリボケーション情報に更新する機能である。CDS1は、RLE41から、新しいリボケーション情報(以下、「新リボケーション情報」という。)を受け取るリボケーション情報受信部14を有している。ここで、RLE41とCDS1間を転送される新リボケーション情報は、例えば、RLE41とCDS1間で予め共有されている暗号鍵を用いて暗号化することにより、転送途上の不当な改変行為から防止されるものとする。

【0028】SMS2は、RLE41が発行する暗号化された新リボケーション情報をリボケーション情報受信部14を通して受け取り、復号した後、リボケーション情報格納部16に格納する。SMS2は、メディア1/F部6に、メモリカード等のPM13が装着された場合に(メディア1/F部6によって装着が検出された場合に)、リボケーション情報格納部16に格納されている新リボケーション情報を当該メディア1/F部6経由で出力する機能を有している。SMS2からPM13への新リボケーション情報の記録は、メディア1/F部6を通じて直接行われるか、またはPD12を経由して行うことができる。

【0029】次にリボケーション情報の種類について説明する。ここで述べるPM13は、音楽コンテンツの記録用としてだけでなく、それ以外のアプリケーションシステム(例えば電子BOOKなど)の記録用としても用いることができる。このとき、各アプリケーションシステムに対応する電子機器の無効化(電子機器が有するアクセス権を無効化すること)を各アプリケーションシステム毎に実施したり管理したりできるようにするために、各アプリケーションシステム毎にリボケーション情報を発行し、各アプリケーションシステム毎に特別に許可された電子機器は、当該アプリケーションシステムに対応するリボケーション情報のみを更新できる。即ち、ここで述べるCDS1は、音楽コンテンツを扱う電子機器(PD、LCM)を対象とするリボケーション情報のみを更新できる。

【0030】これにより、万一、CDS1のリボケーショ

ン更新機能が改変され悪用されることがあっても、他のアプリケーションシステムへ影響を及ぼすことはない

(即ち、他のアプリケーションシステムにおけるリポケーション情報の不当な更新は防止できる)。また、CDS 1のように、リポケーション情報の更新を特別に許可された電子機器についても、PM 13に登録された特別なリポケーション情報(以下、「マスタリポケーション情報」という。)によって、無効化できるようにしている。つまり、リポケーション情報を更新することが許可された特別な電子機器を示すマスタリポケーション情報が、不正にリポケーション情報を改変する電子機器を知るためのブラックリストとして、この著作権保護システム100に導入されている。

【0031】例えば、ある特定のCDS1のリポケーション更新機能が改変され悪用されることがあっても、そのような不正なCDS1の識別情報をマスタリポケーション情報として登録しておくことで、そのCDS1によるリポケーション情報へのアクセスを排除することができるので、リポケーション情報の不正な改ざんを防止することができる。

【0032】なお、本実施例では、マスタリポケーション情報については、本発明の方法で更新することは考えないものとする。マスタリポケーション情報の更新は、新しいマスタリポケーション情報が登録された記憶媒体を発行し、古いマスタリポケーション情報が登録された記憶媒体から、この新しいマスタリポケーション情報が登録された記憶媒体に置き換えていくことによって実現するものとする。

【0033】図2中のPD(記録再生装置)12のブロック構成図

図3は、PM13の構成を示す機能ブロック図である。PM13は、コントローラ130と、公開領域131及び秘匿領域134からなる記憶メディア部とから構成される。秘匿領域134は、コントローラ130を通して非公開の手順(つまり秘匿された特定手続)でしかアクセスできない論理的な記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域134は、秘密の定数(例えば後述するマスタメディア固有鍵KM-M等)が記憶される秘匿ROM領域135と、秘密の変数(例えば後述するライセンスする側から提供されるライセンス復号キーや、暗号化されたコンテンツ復号キー、メディア固有鍵KM-1等)が記憶される秘匿R/W(リード/ライト)領域136からなる。ここで暗号化されたコンテンツ復号キー(以下、単に、「暗号化コンテンツキー」という。)は、コンテンツCを復号するための(当該コンテンツCに固有の)コンテンツキーKCを、PM13に固有のメディア固有鍵KM-1で暗号化することで取得されるものである。

【0034】またマスタメディア固有鍵KM-Mや、メディア固有鍵KM-1は、各PM13に固有であればよく、シリ

アル番号や製造番号(PM13個々の製造番号、または製造ロット番号)、他様々な識別情報を用いることができる。なお、KM-MやKM-1を、前述のPM13に固有な識別情報とライセンス復号キーから生成するようにしても構わない。物理的には、秘匿ROM領域135は、例えばROM(読み出し専用不揮発メモリ)上に確保され、秘匿R/W領域136は、例えばフラッシュメモリ(書換え可能な不揮発性メモリ)の特定領域に確保される。

【0035】公開領域131は、秘匿領域以外の、通常の手順でアクセス可能な論理的な領域であり、読み出し専用の公開領域である公開ROM領域132と、書換え可能な公開領域である公開R/W領域133からなる。但し、公開ROM領域132には、図4に示されるように、非公開の手順で(つまり秘匿された特定手続)でのみ書き換えできる領域である公開ROM-W領域132aを含むものとする。

【0036】図4は、記憶メディア(PM)の公開ROM領域の構成と記憶内容を示す図である。物理的には、公開ROM領域132は、例えばROM上に確保され、公開R/W領域133、及び公開ROM-W領域132aは、例えばフラッシュメモリ上に確保される。なお、この公開ROM領域132、公開ROM-W領域132a、公開R/W領域133は、先の秘匿ROM領域135が確保されるROM、秘匿R/W領域136が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。

【0037】公開ROM領域132のうち公開ROM-W領域132aを除く領域(以下、単に、「公開ROM領域132」という。)には、マスタリポケーション情報(RL-M)が、PM13の出荷段階で予め登録されている。また、公開ROM-W領域132aには、(1つ以上の)リポケーション情報(RL-1、RL-2...)が、PM13の出荷段階で予め登録されている。リポケーション情報については、CDS1等のリポケーション情報更新機能の実行により、新リポケーション情報が、PM13のコントローラ130を通して秘匿の手順で、この公開ROM-W領域132aに登録(更新)される。なお、公開ROM領域132に、本発明の方法により更新することを必要としない別の(1つ以上の)リポケーション情報を予め登録していても構わない。

【0038】本実施の形態において、マスタリポケーション情報、及び、(1つ以上の)リポケーション情報は、具体的には、無効化すべき電子機器の識別情報(64ビットのデバイスID)のリストである。そこで、以下の説明では、「リポケーション情報」に代えて「リポケーションリストRL」なる用語を用いる。以下、マスタリポケーションリストをRL-M、(1つ以上の)リポケーション情報を、アプリケーションごとにRL-1、RL-2...と記述し、その中でRL-1を音楽コンテンツの記録再生に対応する電子機器(PD、LCM等)の無効化に利用されるリポケーションリストとする。

【0039】公開R/W領域133には、暗号化コンテンツ等が適宜記憶されている。この暗号化コンテンツは、コンテンツをコンテンツキーKCで暗号化することで取得されるものである。図5は、CDS1の論理的な記憶領域を示す図である。CDS1は、公開ROM領域112及び公開R/W領域113からなる公開領域111と非公開の手順でしかアクセスできない秘匿領域114との各記憶領域を有している。

【0040】公開R/W領域113には、図2に示す音楽データ格納部10が確保されている。公開ROM領域112には、公開ROM-W領域が含まれており、この公開ROM-W領域に、図2に示すリボケーション情報格納部16が確保されている。(即ち、図2のSMS2は、RLE41から受け取った暗号化された新リボケーション情報を復号し、秘匿の手順で、復号された新リボケーション情報をこの公開ROM-W領域に格納する。

【0041】秘匿領域114には、識別情報(デバイスID) ID\_CDSが予め記憶されている。秘匿領域114には、また各コンテンツ毎のコンテンツキーKCが適宜記憶されている。また、この秘匿領域114に、図2に示す宿帳格納部8が確保されている。ここでSMS2の管理下にある音楽データ格納部10(公開R/W領域113)に保持されている全ての音楽コンテンツは、その識別情報であるコンテンツID(TID)等をその属性として持つ。この属性情報を宿帳と呼び(秘匿領域114内の)宿帳格納部8に格納される。

【0042】CDS1は、それぞれのSMS2によって宿帳格納部8にアクセスするための秘匿された特定の手続きが行われた後、宿帳格納部8(を提供する秘匿領域114)からデータを読み取るための秘匿領域ドライバ7を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。PD12は公開のROM領域122及び公開R/W領域123からなる公開領域121と非公開の手順でしかアクセスできない秘匿領域124との各記憶領域を有している。秘匿領域124には、PD12の識別情報ID\_PDが予め固定記憶されている。秘匿領域124にはまた、各コンテンツ毎のコンテンツキーKCが適宜記憶されている。

【0043】図6は、PD12の構成を示すブロック図である。図7は、PD12の論理的な記憶領域を示す図である。PD12は、半導体プレーヤ等であり、ハードウェア的には、CPU12a、RAM12b、ROM12c、フラッシュメモリ12d、外部機器I/F部12e、メディアI/F部12f、暗号化音楽コンテンツを復号等するための復調部12g、圧縮音楽コンテンツを伸長等するためのデコーダ部12h及びD/A変換部12iから構成され、論理的な記憶領域として、図7に示されるように、公開領域121と秘匿領域124とを有する。

【0044】図6に示されるように、PM13は、PD12のメディアI/F部12fに装着して利用される。CDS1

は、PD12を介してPM13に読み書きする場合は、CDS1内のPD\_I/F部5、PD12内の外部機器I/F部12e、メディアI/F部12fを経由して当該PM13の秘匿領域134(図3参照)にアクセスする。メディアI/F部12fは、PM13の秘匿領域134にアクセスするための秘匿領域アクセス部(図示せず)を有している。PD12内の公開R/W領域123及び秘匿領域124は、例えばフラッシュメモリ上に確保されている。また公開ROM領域122は、ROM12c上に確保されている。このROM12cには、PM13との間で相互認証を行うためのプログラムが書き込まれている。PD12では、CPU12aの制御のもと、このプログラムに従ってPM13との間の相互認証等の処理が実行される。

【0045】図8は、LCM21の構成を示すブロック図である。LCM21は、例えば、パーソナルコンピュータを用いて実現され、リボケーション情報の更新機能を有さない点を除けば、基本的にCDS1と同様の構成、即ち、SMS22、EMD\_I/F部23、PD\_I/F部25、メディアI/F部26、秘匿領域ドライバ27、宿帳格納部28、ライセンス格納部29、音楽データ格納部30、CD\_I/F部31及びユーザI/F部35を備える。

【0046】したがって、LCM21は、CDS1と同様に、EMD40から暗号化コンテンツを受け取り、LCM21上に保管したり、LCM21上に保管された暗号化コンテンツを、記憶媒体PM13に記録したり、記憶媒体PM13上の音楽コンテンツをLCM21上に移動保管するための機能を有している。図9は、LCM21の論理的な記憶領域を示す図である。PM13、CDS1、PD12と同様に、LCM21は、公開のROM領域212及び公開R/W領域213からなる公開領域211と非公開の手順でしかアクセスできない秘匿領域214との各記憶領域を有している。秘匿領域214には、LCM21の識別情報ID\_LCMが予め固定記憶されている。秘匿領域214にはまた、各コンテンツ毎のコンテンツキーKCが適宜記憶されている。

【0047】PM13は、LCM21のメディアI/F部26に装着して利用される。LCM21がPM13へ読み書きする場合は、LCM21内のメディアI/F部26を経由して当該PM13の秘匿領域134にアクセスする。メディアI/F部26は、PM13の秘匿領域134にアクセスするための秘匿領域アクセス部(図示せず)を有している。LCM21内の公開R/W領域213及び秘匿領域214は、例えばフラッシュメモリ上に確保されている。また公開ROM領域212は、ROM上に確保されている。このROMにはPM13との間で相互認証を行うためのプログラムが書き込まれている。LCM21では、CPU(図示せず)の制御のもと、このプログラムに従ってPM13との間の相互認証等の処理が実行される。

【0048】次に、本実施の形態における著作権保護システム100の動作について、利用者が、PM13を、CDS1に挿入し、あるEMD40で配信された音楽コンテンツ

を、PM13に記録（購入）する処理を選択した場合に、RLE（RLE41）が発行し、CDS1によって既に保持されている新リボケーション情報が、当該音楽コンテンツとともに、PM13に記録されるとき動作を例に、説明する。

【0049】図10及び図11は、それぞれ、そのようなケースにおけるCDS1とPM13間での通信と処理の流れにおける前半及び後半を示す図である。音楽コンテンツの購入指示が例えばCDS1のユーザインターフェース（I/F部）15を介してなされ、かつ、PM13がCDS1のメディアI/F部6に装着されたことが相互で検出された後に、CDS1のメディアI/F部とPM13のコントローラ130との間で周知の相互認証（AKE（AUTHENTICATION AND KEY EXCHANGE）-M（MASTER））が行われる（ステップS101）。この相互認証AKE-Mは、例えばCDS1とPM13の間で、次のように行われる。

【0050】まず、CDS1からPM13を認証する。ここで（リボケーションの更新を許可された特別の）CDS1は認証鍵K1-Mを保持しており、PM13は、同じ認証鍵K1-Mを保持している（図示していないがいずれも秘匿ROM領域の保持されている）。CDS1は乱数R1を発生してPM13に送る。PM13は、CDS1で発生された乱数R1を受け取ると、それを認証鍵K1-Mで暗号化して、その暗号化された乱数（K1-M[R1]）を表す）をCDS1に返す。CDS1では、認証鍵K1-Mを用いて、K1-M[R1]を復号し、復号結果が先に発生した乱数R1に等しければ、PM13は正しい相手であると判定する。

【0051】その後、上記と同じことをPM13からCDS1に対して行うことで、相互認証を行う。この場合、CDS1、PM13はそれぞれ認証鍵K2-Mを保持し、CDS1がPM13で発生した乱数R2をK2-Mで暗号化してそれをPM13でK2-Mを用いて復号し、先に発生した乱数R2に等しいかを確認する。ここで、認証鍵K1-M、K2-Mは、リボケーションの更新を許可された特別の電子機器（ここではCDS1）にのみ与えることにより、一般の電子機器（LCM21など）による認証処理AKE-Mを行うことを防止することができる。

【0052】以上の相互認証AKE-M（S101）により、CDS1及びPM13が双方で正当な相手であることが確認されたとき、CDS1のメディアI/F部とPM13のコントローラ130との間でキー交換が行われ、同一のセッション鍵（KY1）が共有される。このセッション鍵KY1は、例えば、上記で相互に発生した乱数R1とR2の排他的論理和値を、CDS1及びPM13が予め共有している秘密鍵生成アルゴリズムに、入力した際の出力値として求められ、従って、セッション鍵KY1は毎回変わる時変キーである。

【0053】CDS1のメディアI/F部6は、秘匿領域114に秘匿（記憶）されている自身のマスタ識別情報ID-Mを読み出して当該ID-Mをセッション鍵KY1で暗号化し、

その暗号化されたID-M（=KY1[ID-M]）をメディアI/F部6からPM13に送る（ステップS102）。PM13のコントローラ130は、CDS1側からのKY1[ID-M]を、先のキー交換で取得したセッション鍵（KY1）で復号し、ID-Mを得る（ステップS103）。

【0054】次にPM13のコントローラ130は、復号したCDS1のマスタ識別情報ID-Mにより、公開ROM132内のマスタリボケーションリストRL-Mを参照し、当該ID-Mに一致する識別情報が登録されているか否かにより、CDS1によるPM13の利用を無効化するか否かを判定する（ステップS104）。もし、ID-Mに一致する識別情報がマスタリボケーションリストRL-Mに登録されている場合には、コントローラ130は該当するCDS1によるPM13の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【0055】これに対し、ID-Mに一致する識別情報がマスタリボケーションリストRL-Mに登録されていない場合は、コントローラ130は該当するCDS1によるPM13の利用（リボケーション情報の更新）が許可されているものと判定し、秘匿ROM領域135に格納されている秘匿されているマスタメディア固有鍵KM-Mを読み出し出力する（ステップS105）。そしてコントローラ130は、CDS1のメディアI/F部6の間で（当該CDS1のメディアI/F部6を介して）キー交換を行い、同一のセッション鍵KY2を共有した上で、上記読み出したマスタメディア固有鍵KM-Mをセッション鍵（KY2）で暗号化し、その暗号化されたKM-M（=KY2[KM-M]）をCDS1に送る（ステップS106）。ここで、セッション鍵KY2は、例えば、先のセッション鍵KY1を、CDS1及びPM13が予め共有している秘密鍵生成アルゴリズムに、入力した際の出力値として求められる。

【0056】CDS1のメディアI/F部6は、PM13側からのKY2[KM-M]を、先のキー交換で取得したセッション鍵（KY2）で復号し、マスタメディア固有鍵KM-Mを得る（ステップS107）。次にCDS1のメディアI/F部6は、公開ROM-W領域に格納されている新リボケーション情報RL-1、及び、メディアI/F部6で生成される新しいメディア固有鍵KM-1Nを取得したマスタメディア固有鍵KM-Mにより暗号化し、その暗号化されたKM-M[RL-M]及びKM-M[KM-1N]をPM13に送る（ステップS108）。

【0057】ここで、メディア固有鍵KM-1Nは、例えば、先のセッション鍵KY2を、CDS1が秘密に保持する鍵生成アルゴリズム入力したときに得られる出力値として生成されるものとする。PM13のコントローラ130は、CDS1側からのKM-M[RL-M]及びKM-M[KM-1N]を、秘匿ROM領域135に格納されたKM-Mを用いて復号し、RL-M、KM-1Nを得る（ステップS109）。

【0058】次に、CDS1のメディアI/F部とPM13のコントローラ130との間で上述した相互認証（AKE-M）と同様の相互認証（AKE-1）が行われる（ステップS1

10)。すなわち、まずは、CDS1からPM13を認証する。ここでCDS1は認証鍵K1-1を保持しており、PM13は、同じ認証鍵K1-1を保持している（図示していないがいずれも秘匿ROM領域の保持されている）。CDS1は乱数R3を発生してPM13に送る。PM13は、CDS1で発生された乱数R3を受け取ると、それを認証鍵K1-1で暗号化して、その暗号化された乱数（K1-1[R3]と表す）をCDS1に返す。CDS1では、認証鍵K1-1を用いて、K1-1[R3]を復号し、復号結果が先に発生した乱数R3に等しければ、PM13は正しい相手であると判定する。

【0059】その後、上記と同じことをPM13からCDS1に対して行うことで、相互認証を行う。この場合、CDS1、PM13はそれぞれ認証鍵K2-1を保持し、CDS1がPM13で発生した乱数R24をK2-1で暗号化してそれをPM13でK2-1で復号し、先に発生した乱数R4に等しいかを確認する。ここで、認証鍵K1-1、K2-1は、音楽コンテンツの利用を許可された電子機器（ここではPD12、LCM21）にのみ与えることにより、他のアプリケーションシステムに対応する電子機器による認証処理AKE-1を行うことを防止することができる。

【0060】以上の相互認証AKE-1（S110）により、CDS1及びPM13が双方で正当な相手であることが確認されたとき、CDS1のメディアI/F部とPM13のコントローラ130との間でキー交換が行われ、同一のセッション鍵（KX1）が共有される。このセッション鍵KX1は、例えば、上記で相互に発生しあった乱数R3とR4の排他的論理和値を、CDS1及びPM13が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められ、従って、セッション鍵KX1は毎回変わる時変キーである。

【0061】CDS1のメディアI/F部6は、秘匿領域114に秘匿（記憶）されている自身の識別情報ID-1を読み出して当該ID-1をセッション鍵KX1で暗号化し、その暗号化されたID-1（=KX1[ID-1]）をメディアI/F部6からPM13に送る（ステップS111）。PM13のコントローラ130は、CDS1側からのKX1[ID-1]を、先のキー交換で取得したセッション鍵（KX1）で復号し、ID-1を得る（ステップS112）。

【0062】次にPM13のコントローラ130は、復号したCDS1の識別情報ID-1により、公開ROM132内のリポケーションリストRL-1を参照し、当該ID-1に一致する識別情報が登録されているか否かにより、CDS1によるPM13の利用を無効化するか否かを判定する（ステップS113）。もし、ID-1に一致する識別情報がリポケーションリストRL-1に登録されている場合には、コントローラ130は該当するCDS1によるPM13の利用を無効化（リポケート）すべきものと判定し、以降の処理を停止する。

【0063】これに対し、ID-1に一致する識別情報が

リポケーションリストRL-1に登録されていない場合は、コントローラ130は該当するCDS1によるPM13の利用（コンテンツの記録）が許可されているものと判定し、ステップS109で得た新リポケーション情報RL-1N、新しいメディア固有鍵KM-1Nによって、RL-1、KM-1をそれぞれ更新する（ステップS114）。

【0064】その後、図11に示されるように、CDS1のメディアI/F部6は、PM13のコントローラ130の間で（当該CDS1のメディアI/F部6を介して）キー交換を行い、同一のセッション鍵KX2を共有した上で、CDS1のメディアI/F部6は、秘匿領域114に秘匿（記憶）されている自身の識別情報ID-1を読み出して当該ID-1をセッション鍵KX2で暗号化し、その暗号化されたID-1（=KX2[ID-1]）をメディアI/F部6からPM13に送る（ステップS115）。ここで、セッション鍵KX2は、例えば、先のセッション鍵KX1を、CDS1及びPM13が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【0065】PM13のコントローラ130は、CDS1側からのKX2[ID-1]を、先のキー交換で取得したセッション鍵（KX2）で復号し、ID-1を得る（ステップS116）。次にPM13のコントローラ130は、復号したCDS1の識別情報ID-1により、公開ROM-W領域内の新リポケーションリストRL-1Nを参照し、当該ID-1に一致する識別情報が登録されているか否かにより、CDS1によるPM13の利用を無効化するか否かを判定する（ステップS117）。

【0066】もし、ID-1に一致する識別情報がリポケーションリストRL-1Nに登録されている場合には、コントローラ130は該当するCDS1によるPM13の利用を無効化（リポケート）すべきものと判定し、以降の処理を停止する。これに対し、ID-1に一致する識別情報がリポケーションリストRL-1Nに登録されていない場合は、コントローラ130は該当するCDS1によるPM13の利用（コンテンツの記録）が許可されているものと判定し、秘匿ROM領域135に格納されている秘匿されているメディア固有鍵KM-1Nを読み出し出力する（ステップS118）。そしてコントローラ130は、CDS1のメディアI/F部6の間で（当該CDS1のメディアI/F部6を介して）キー交換を行い、同一のセッション鍵KX3を共有した上で、上記読み出したメディア固有鍵KM-1Nをセッション鍵（KX3）で暗号化し、その暗号化されたKM-1N（=KX3[KM-1N]）をCDS1に送る（ステップS119）。ここで、セッション鍵KX3は、例えば、先のセッション鍵KX2を、CDS1及びPM13が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【0067】CDS1のメディアI/F部6は、PM13側からのKX3[KM-1N]を、先のキー交換で取得したセッション鍵（KX3）で復号し、メディア固有鍵KM-1Nを得る（ス

テップS120)。次にCOS1のメディアI/F部6は、秘匿領域114に秘匿されているコンテンツキーKCを取得したメディア固有鍵KM-1Nにより暗号化し、暗号化されたKM-1N[KC]をPM13の秘匿R/W領域に送る(ステップS121)。

【0068】また、COS1のメディアI/F部6は、公開R/W領域113に格納されている暗号化コンテンツKC[C]を、PM13の公開R/W領域に送る(ステップS122)。このように、本実施の形態では、マスタリボケーションリストRL-Mに従って無効化(リボケート)されたならば渡ることのない(暗号化された)マスタメディア固有鍵KM-Mを当該PM13からCOS1が受け取り、そのCOS1の公開ROM領域114に格納されている新リボケーション情報RL-1、及び、メディア固有鍵KM-1Nを当該マスタメディア固有鍵KM-Mにより暗号化し、PM13に送るようにしている。

【0069】このため、マスタリボケーションリストRL-Mで指定される無効化対象COS(PM13のリボケーション情報を更新しようとする電子機器)を確実に無効化(排除)できる。さらにリボケーションリストRL-1に従って無効化(リボケート)されたならば、PM13において、新リボケーション情報RL-1及びメディア固有鍵KM-1Nへの更新を行わない様にしている。さらに、新リボケーションリストRL-1Nに従って無効化(リボケート)されたならば渡ることのない(暗号化された)メディア固有鍵KM-1を当該PM13からCOS1が受け取り、そのCOS1の秘匿領域114に格納されているコンテンツキーKCを当該メディア固有鍵KM-1Nにより暗号化し、PM13に送るようにしている。このため、新リボケーションリストRL-1Nで指定される無効化対象COS1(PM13を利用しようとする電子機器)を確実に無効化(排除)できる。

【0070】次に、PM13に格納された暗号化コンテンツをPD12上で復号して再生する場合の動作について、説明する。なお、以下の説明では、PD12上で復号して再生する場合を例に説明するが、LCM21上で復号して再生する場合も全く同じ手順で行われる。図12は、そのようなケースにおけるPM13とPD12間での通信と処理の流れを示す図である。

【0071】まず、再生指示が例えばPD12に対してなされ、かつPM13がPD12のメディアI/F部12fに装着された段階で、PD12のCPU12aとPM13のコントローラ130との間で(前記S110と同様の)相互認証AKE-1が行われる(ステップS201)。そして、この相互認証(S201)によりPD12及びPM13の双方で正当な相手であることが確認されたとき、PD12のCPU12aとPM13のコントローラ130との間でキー交換が行われ同一のセッション鍵(KX4)が共有される。

【0072】PD12のCPU12aは、秘匿領域124に秘匿されている自身の識別情報ID-PDを読み出して当該I

D-PDをセッション鍵(KX4)で暗号化し、その暗号化されたID-PD(=KX4[ID-PD])をメディアI/F部12fからPM13に送る(ステップS202)。PM13のコントローラ130は、PD12側からおくKX4[ID-PD]を、先のキー交換で取得したセッション鍵(KX4)で復号し、ID-PDを得る(ステップS203)。

【0073】PM13のコントローラ130は、復号したPD12の識別情報ID-PDにより公開ROM-W領域内のリボケーションリストRL-1Nを参照し、当該ID-PDに一致する識別情報が登録されているか否かにより、PD12によるPM13の利用を無効化するか否かを判定する(ステップS204)。もし、ID-PDに一致する識別情報がリボケーションリストRL-1Nに登録されている場合には、コントローラ130は該当するPD12によるPM13の利用を無効化(リボケート)すべきものと判定し、以降の処理を停止する。

【0074】これに対し、ID-PDに一致する識別情報がリボケーションリストRL-1Nに登録されていない場合は、コントローラ130は該当するPD12によるPM13の利用が許可されているものと判定し、秘匿R/W領域136に秘匿されているメディア固有鍵KM-1Nを読み出し出力する(ステップS205)。そしてコントローラ130は、PD12のCPU12aとの間で(当該PD12のメディアI/F部12fを介して)キー交換を行い、同一のセッション鍵(KX5)を共有した上で、上記読み出したメディア固有鍵(KX5)で暗号化し、その暗号化されたKM-1N(=KX5[KM-1N])をPD12に送る(ステップS206)。ここで、セッション鍵KX5は、例えば、先のセッション鍵KX4を、PD12及びPM13が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【0075】PD12のCPU12aは、PM13側からのKX5[KM-1N]を、先のキー交換で取得したセッション鍵(KX5)で復号し、メディア固有鍵KM-1Nを得る(ステップS207)。次に、PD12のCPU12aは、PM13の秘匿R/W領域136に記憶されている暗号化コンテンツKC(=KM-1N[KC])を読み込んで、ステップS207で取得したメディア固有鍵KM-1Nにより復号する(ステップS208)。次に、PD12のCPU12aは、PM13の公開R/W領域133に記憶されている暗号化コンテンツC(=KC[C])を読み込んで、ステップS208で取得したコンテンツキーKCにより復号して再生する(ステップS2089)。

【0076】このように、本実施の形態では、リボケーションリストRL-1Nに従って、無効化(リボケート)されたならばPM13から渡されることのない(暗号化された)メディア固有鍵KM-1Nを当該PM13からPD12が受け取り、当該PM13の秘匿R/W領域に秘匿されている暗号化コンテンツキー(KM-1N[KC])をそのメディア固有鍵KM-1Nにより復号し、PD12での暗号化コンテンツの



復号に利用するようにしている。このため、新リボケーションリストRL-1Nで指定される無効化対象PD(PM13を利用しようとする電子機器)を確実に無効化できる。

【0077】以上、本発明に係る著作権保護システム100について、実施の形態に基づいて説明したが、本発明は、この実施の形態に限られないことは勿論である。例えば、本実施の形態では、著作権保護の対象となるデジタル著作物は、音楽コンテンツであったが、映画やゲームソフト等のデータであってもよい。また、本実施の形態では、CDS1とPM13の間、PD12とPM13の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報をセッション鍵(KYI、KXI)により暗号化するものとしたが、暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものにするためには、セッション鍵による暗号化を行うことが望ましい。

【0078】また、本実施の形態では、マスターボケーションリストRL-M、及びリボケーションリストRL-1、RL-1Nが公開ROM領域132(あるいは公開ROM-W領域)に登録されているものとして説明したが、リボケーションリストが改竄されない領域であれば良く、例えば秘匿された特定の手続きでしかアクセスできない秘匿領域134に登録されるようにしてもよい。

【0079】また、本実施の形態では、暗号化コンテンツキー(KM-1N[KC])は、秘匿R/W領域136に格納されるものとして説明したが、公開R/W領域133に格納されるようにしてもよい。また、本実施の形態では、電子機器の識別情報は、電子機器から記憶媒体に転送されたが、本発明は、そのような転送方向に限定されるものではなく、逆の転送方向であってもよい。

【0080】例えば、記憶媒体は、リボケーション情報として、コンテンツへのアクセスを許可する電子機器については、所定の第1鍵K1をその電子機器の識別情報IDで暗号化して得られる値E(ID,K1)を記憶しておき、一方、コンテンツへのアクセスを禁止する電子機器については、所定の第2鍵K2をその電子機器の識別情報IDで暗号化して得られる値E(ID,K2)を記憶しておく。

【0081】そして、記憶媒体が電子機器に装着されると、まず、記憶媒体は、上述のようなリボケーション情報Eと乱数Rを電子機器に送信する。それらE及びRを受け取った電子機器は、リボケーション情報Eを自分の識別情報IDで復号することによって、無効化されていない場合には、第1の鍵K1を取得し、一方、無効化されている場合には、第2の鍵K2を取得する。そして、取得した鍵K(K1又はK2)を乱数Rで暗号化し、得られた値E(K,R)を記憶媒体に返信する。

【0082】記憶媒体は、受け取った値E(K,R)を復号し、得られた乱数R'と、電子機器に送信しておいた乱数Rとを比較し、一致する場合にのみ、コンテンツへのアクセスを許可すればよい。マスターボケーション情報に

についても、同様の記憶内容と手順にすることで、電子機器の識別情報の転送方向を反転させることができる。

【0083】

【発明の効果】以上の説明から明らかなように、電子機器に装着されて使用される記憶媒体であって、デジタルコンテンツを記憶するためのコンテンツ記憶領域と、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報に対応する情報をリボケーション情報として記憶するためのリボケーション情報記憶領域と、前記リボケーション情報記憶領域に記憶されるリボケーション情報の更新を禁止する対象となる電子機器の識別情報に対応する情報をマスターボケーション情報として記憶しているマスターボケーション情報記憶領域とを備えることを特徴とする。

【0084】これによって、権限なくリボケーション情報を更新しようとする不正な電子機器の識別情報に対応する情報については、その記憶媒体のマスターボケーション情報記憶領域に予め登録しておくことができるので、この情報を参照することで、リボケーション情報にアクセスしようとした電子機器が正当な電子機器であるか不正な電子機器であるかを知ることができる。

【0085】したがって、リボケーション情報は、安全性が保証された書き換え可能な記憶領域に保管されるので、後発的に不正な電子機器が出現しても、その電子機器の識別情報に対応する情報をリボケーション情報記憶領域に追加登録することで、それ以降におけるデジタル著作物への不正なアクセスが排除される。ここで、前記記憶媒体は、さらに、当該記憶媒体が装着された電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへの前記電子機器によるアクセスを許可するコンテンツ保護手段と、前記電子機器の識別情報が前記マスターボケーション情報記憶領域に記憶されたマスターボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記電子機器からの指示に従って、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新するリボケーション情報更新手段とを備えてもよい。

【0086】これによって、マスターボケーション情報記憶領域に登録されていない識別情報を有する電子機器だけが、その記憶媒体のリボケーション情報を更新することが許可されるので、不正な電子機器によるリボケーション情報の改ざんが防止される。また、前記マスターボケーション情報記憶領域は、予めマスターボケーション情報が記憶されたROMとしてもよい。これによって、記憶媒体が出荷された後においてマスターボケーション情報自体を改ざんする、という攻撃に備えることが



できる。

【0087】また、前記記憶媒体は、さらに、前記リボケーション情報更新手段によるリボケーション情報の更新の許否判断に先立って、前記電子機器と相互認証をし、相互認証に成功した場合にのみ前記電子機器と共有し合うことができる秘密鍵を生成する相互認証手段を備え、前記リボケーション情報更新手段は、前記相互認証手段が生成した秘密鍵を用いて前記リボケーション情報を更新してもよい。

【0088】これによって、リボケーション情報を更新する権限に関わる極めて重要な識別情報は、秘匿化された状態で記憶媒体と電子機器間で転送されるので、リボケーション情報の改ざんに対する防御が強化される。また、前記リボケーション情報更新手段は、前記識別情報が前記マスタリボケーション情報に対応する識別情報に該当しないと判断した場合には、前記電子機器がリボケーション情報を更新するために必要となる秘密鍵を前記電子機器に送信してもよい。

【0089】これによって、リボケーション情報の更新権限の有無に関する判断結果が秘匿化され、それら装置間を盗聴する不正行為に備えることができる。また、前記リボケーション情報記憶領域は、複数のグループに分類してリボケーション情報を記憶するための複数の記憶領域を有し、前記リボケーション情報更新手段は、当該記憶媒体に装着された電子機器の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しないと判断し、かつ、前記電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたりボケーション情報のうち前記電子機器が更新しようとしているグループに属するリボケーション情報に対応する識別情報に該当しないと判断した場合に、前記グループに属するリボケーション情報だけを更新してもよい。

【0090】これによって、リボケーション情報が不正に改ざんされるという攻撃を受けた場合であっても、他のアプリケーションシステムはその影響を受けないので、被害は最小限に抑えられる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態における著作権保護システムの全体構成を示す概観図である。

【図2】コンテンツ販売システム（CONTENT DISTRIBUTE SYSTEM（CDS））の構成を示すブロック図である。

【図3】記憶メディア（PORTABLE MEDIA（PM））の構成

を示すブロック図である。

【図4】記憶メディア（PM）の公開ROM領域の構成と記憶内容を示す図である。

【図5】CDSの論理的な記憶領域を示す図である。

【図6】記録再生装置（PORTABLE DEVICE（PD））の構成を示すブロック図である。

【図7】PDの論理的な記憶領域を示す図である。

【図8】コンテンツ利用管理システム（LICENSE COMPLIANT MODULE（LCM））の構成を示すブロック図である。

10 【図9】LCMの論理的な記憶領域を示す図である。

【図10】CDSとPM間での通信と処理の流れにおける前半を示す図である。

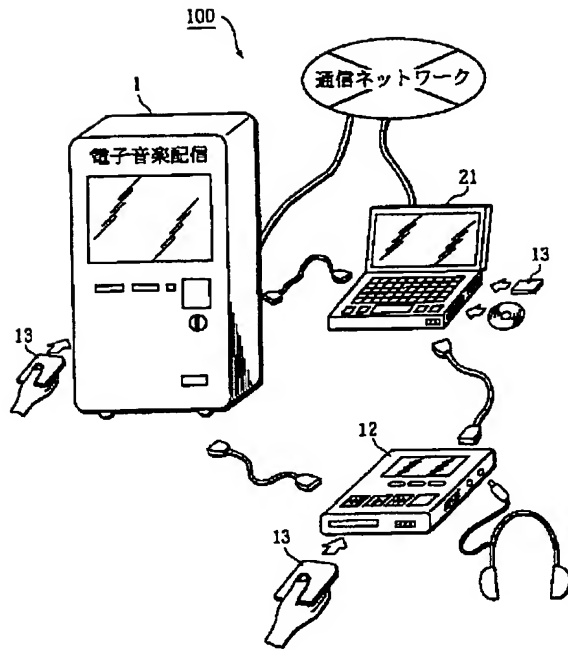
【図11】CDSとPM間での通信と処理の流れにおける後半を示す図である。

【図12】PMとPD間での通信と処理の流れを示す図である。

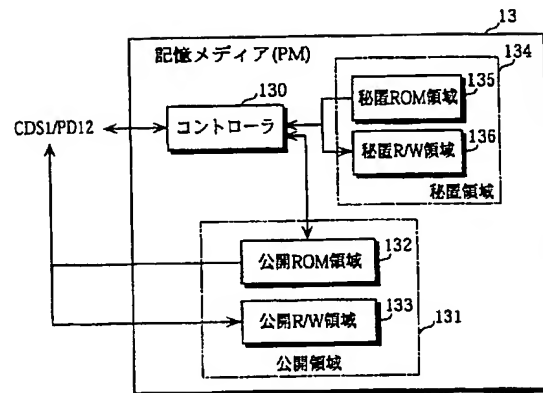
#### 【符号の説明】

- |    |                 |                     |  |
|----|-----------------|---------------------|--|
|    | 1               | コンテンツ販売システム（CDS）    |  |
|    | 2、22            | セキュア・コンテンツ・サーバ（SMS） |  |
| 20 | 3、23            | EMD_I/F部            |  |
|    | 5、25            | PD_I/F部             |  |
|    | 6、26            | メディア_I/F部           |  |
|    | 7、27            | 秘匿領域ドライバ            |  |
|    | 8、28            | 宿帳格納部               |  |
|    | 9、29            | ライセンス格納部            |  |
|    | 10、30           | 音楽データ格納部            |  |
|    | 12              | 記録再生装置（PD）          |  |
|    | 13              | 記憶メディア（PM）          |  |
|    | 14              | リボケーション情報受信部        |  |
| 30 | 15、35           | ユーザ_I/F部            |  |
|    | 16              | リボケーション情報格納部        |  |
|    | 21              | コンテンツ利用管理システム（LCM）  |  |
|    | 31              | CD_I/F部             |  |
|    | 100             | 著作権保護システム           |  |
|    | 111、121、131、211 | 公開領域                |  |
|    | 112、122、132、212 | 公開ROM領域             |  |
|    | 132a            | 公開ROM-W領域           |  |
|    | 113、123、133、213 | 公開R/W領域             |  |
|    | 114、124、134、214 | 秘匿領域                |  |
| 40 | 130             | コントローラ              |  |
|    | 134             | 秘匿領域                |  |
|    | 135             | 秘匿ROM領域             |  |
|    | 136             | 秘匿R/W領域             |  |

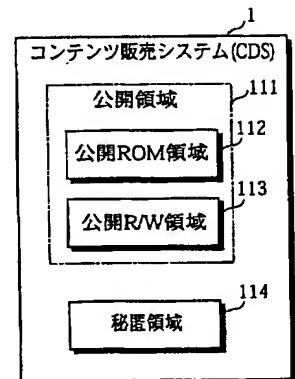
【図1】



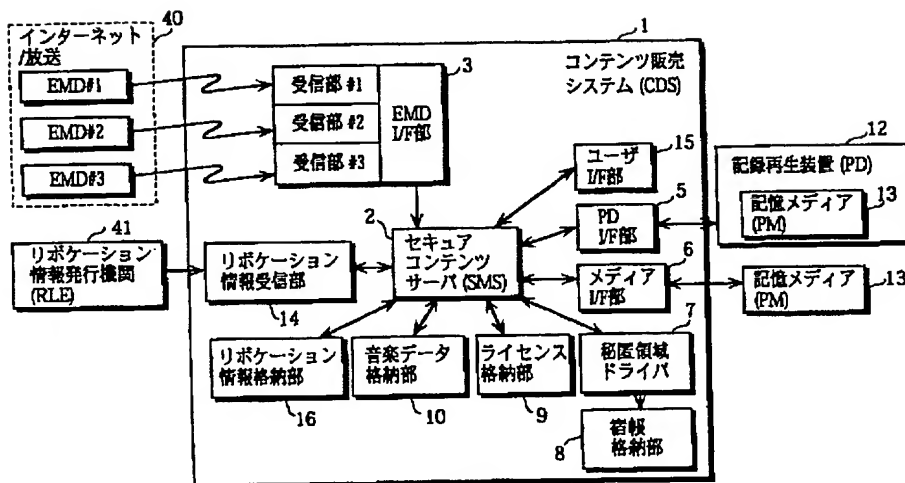
【図3】



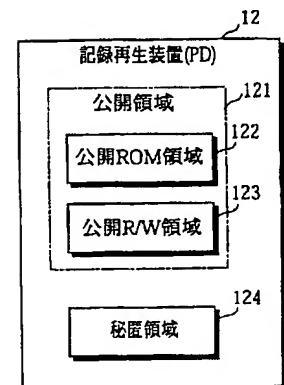
【図5】



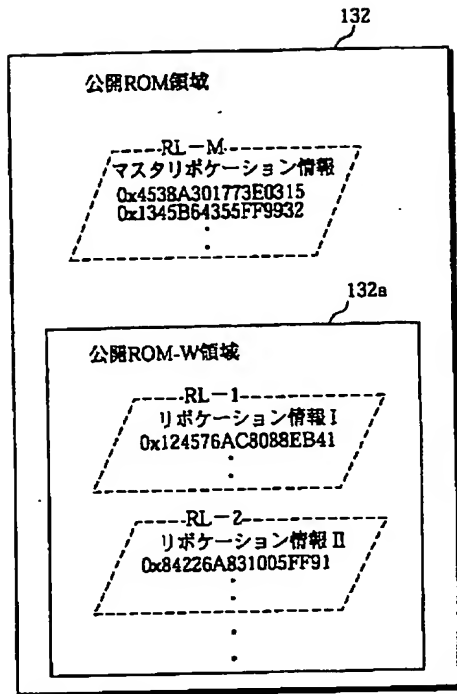
【図2】



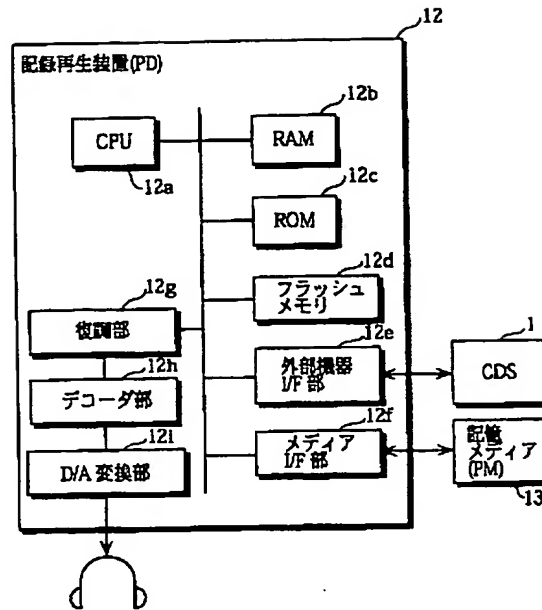
【図7】



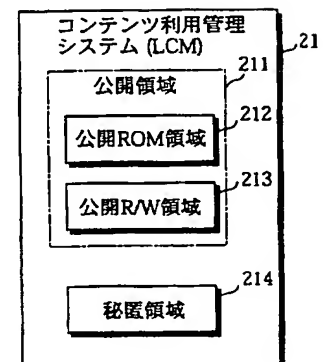
【図4】



【図6】



【図9】



【図8】

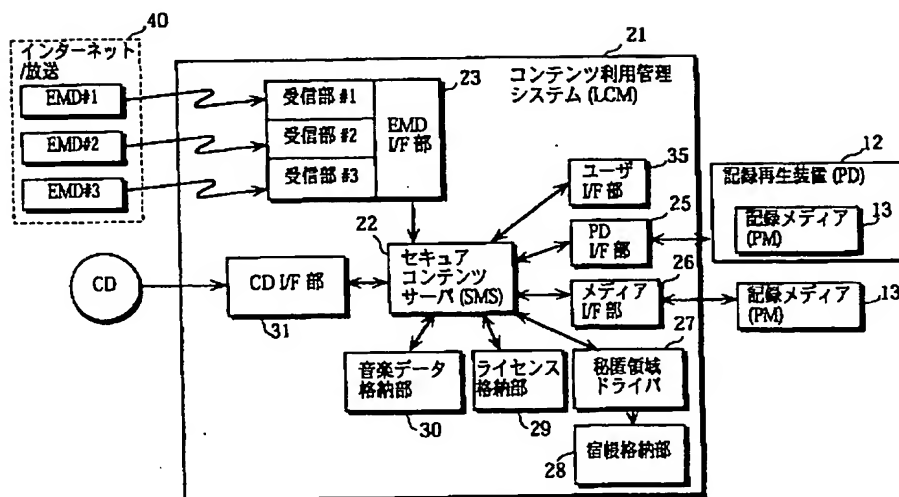


Figure 1 is a block diagram of a content distribution system (CDS) and its connection to a controller and memory media. The system is divided into three main sections: the CDS (1), the Controller (13), and the Memory Media (PM).

**Content Distribution System (CDS) (1):**

- Secret Key Area (秘密領域):** Contains **ID-M** and **RL-1N** (Public ROM-W Area).
- Public ROM-W Area (公開ROM-W領域):** Contains **KM-IN** (Secret Key Area).
- Secret Key Area (秘密領域):** Contains **ID-1**.
- Processors:** **AKE-M** (Key Agreement), **E** (Encryption), **D** (Decryption), **SW** (Switch), and **判定** (Judgment).
- Connections:** **ID-M** is connected to **E**. **RL-1N** is connected to **D**. **KM-IN** is connected to **E**. **ID-1** is connected to **E**. **AKE-M** is connected to **E** and **D**. **E** is connected to **D**. **D** is connected to **SW**. **SW** is connected to **判定**. **判定** is connected to **SW**.
- Signals:** **S101** (AKE-M to D), **S102** (E to D), **S103** (D to SW), **S104** (SW to 判定), **S105** (SW to 判定), **S106** (D to SW), **S107** (D to E), **S108** (E to D), **S109** (D to SW), **S110** (AKE-1 to D), **S111** (E to D), **S112** (D to SW), **S113** (SW to 判定), **S114** (SW to 判定).

**Controller (13):**

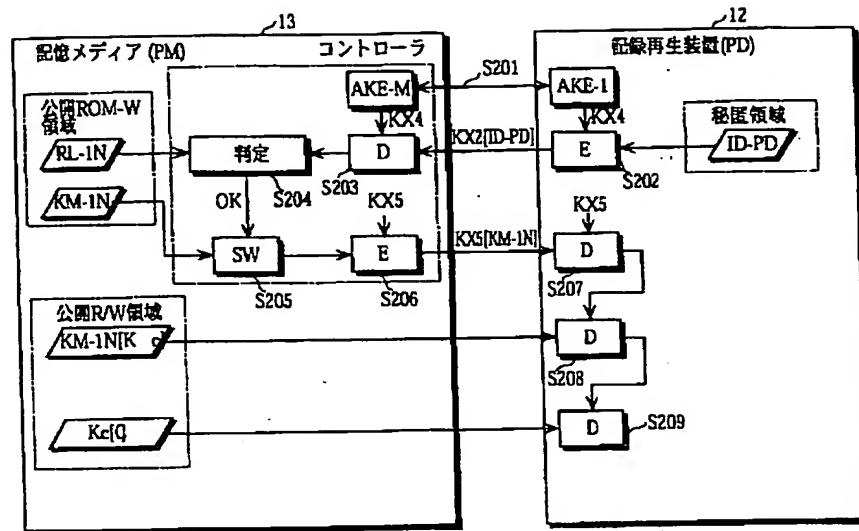
- Secret Key Area (秘密領域):** Contains **ID-M** and **RL-1N** (Public ROM-W Area).
- Public ROM-W Area (公開ROM-W領域):** Contains **KM-M** (Secret Key Area).
- Secret Key Area (秘密領域):** Contains **ID-1**.
- Processors:** **AKE-M** (Key Agreement), **E** (Encryption), **D** (Decryption), **SW** (Switch), and **判定** (Judgment).
- Connections:** **ID-M** is connected to **E**. **RL-1N** is connected to **D**. **KM-M** is connected to **E**. **ID-1** is connected to **E**. **AKE-M** is connected to **E** and **D**. **E** is connected to **D**. **D** is connected to **SW**. **SW** is connected to **判定**. **判定** is connected to **SW**.
- Signals:** **S101** (AKE-M to D), **S102** (E to D), **S103** (D to SW), **S104** (SW to 判定), **S105** (SW to 判定), **S106** (D to SW), **S107** (D to E), **S108** (E to D), **S109** (D to SW), **S110** (AKE-1 to D), **S111** (E to D), **S112** (D to SW), **S113** (SW to 判定), **S114** (SW to 判定).

**Memory Media (PM):**

- Secret Key Area (秘密領域):** Contains **ID-M** and **RL-1N** (Public ROM-W Area).
- Public ROM-W Area (公開ROM-W領域):** Contains **KM-M** (Secret Key Area).
- Secret Key Area (秘密領域):** Contains **ID-1**.
- Processors:** **AKE-M** (Key Agreement), **E** (Encryption), **D** (Decryption), **SW** (Switch), and **判定** (Judgment).
- Connections:** **ID-M** is connected to **E**. **RL-1N** is connected to **D**. **KM-M** is connected to **E**. **ID-1** is connected to **E**. **AKE-M** is connected to **E** and **D**. **E** is connected to **D**. **D** is connected to **SW**. **SW** is connected to **判定**. **判定** is connected to **SW**.
- Signals:** **S101** (AKE-M to D), **S102** (E to D), **S103** (D to SW), **S104** (SW to 判定), **S105** (SW to 判定), **S106** (D to SW), **S107** (D to E), **S108** (E to D), **S109** (D to SW), **S110** (AKE-1 to D), **S111** (E to D), **S112** (D to SW), **S113** (SW to 判定), **S114** (SW to 判定).

Figure 1 is a block diagram of a content distribution system (CDS) and a controller. The CDS (left) includes a '秘匿領域' (Secret Area) with 'ID-1' and 'Kc', and a '公開R/W領域' (Public R/W Area) with 'Kc[C]'. The Controller (right) includes a 'コントローラ' (Controller) with 'D', 'E', 'JUDGEMENT', and 'SW' blocks, and a '記憶メディア (PM)' (Storage Media) with '公開R/W領域' (Public R/W Area) containing 'RL-IN' and 'KM-IN', and a '秘匿R/W領域' (Secret R/W Area) containing 'KM-IN[K]' and 'Kc[C]'. Data flows are indicated by arrows with labels like KX2, KY1, ID-1, KX3, S115, S116, S117, S118, S119, S120, S121, S122, and KM-M.

【図12】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

H04L 9/32

識別記号

FI

H04L 9/00

テマコード(参考)

673B

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 小塚 雅之

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 廣田 照人

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(72)発明者 田村 正文

東京都港区芝浦一丁目1番1号 株式会社  
東芝本社事務所内

This Page Blank (uspto)